01net

OK

nos newsletters

nos magazines

01net Lisez **01net** pour 2,45 € / n° seulement



# Black Hat 2014: Bienvenue à Las Vegas, entre hackers paranos et espions pas réglos

**Les conférences de sécurité BlackHat et Defcon ouvrent leurs portes cette semaine dans la ville des casinos. 01net sera sur place, à ses risques et périls comme le précisent les organisateurs.**

Gilbert Kallenborn | 01net | le 05/08/14 à 08h07 | laisser un avis

Tweet

agrandir la photo

Jusqu'à dimanche prochain, Las Vegas est la capitale de la sécurité informatique, car c'est dans la cité du péché que se déroulent à nouveau les deux conférences les plus importantes en la matière : BlackHat du 2 au 7 août, suivi de Defcon du 7 au 10. A cette occasion, *01net* se rend sur place pour couvrir les annonces les plus importantes et donner un aperçu *in vivo* de ces deux rassemblements où se côtoient hackers, pirates, policiers, espions, militaires et autres experts en sécurité en tous genres.

Face à un tel méli-mélo, la parano est évidemment de rigueur à Las Vegas. D'ailleurs, les organisateurs ne s'en cachent pas et éditent des listes de bons conseils pour tous ceux qui ne seraient pas habitués à l'esprit taquin qui règne dans ce milieu. C'est le cas par exemple des journalistes, qui ne sont généralement pas rompus aux technologies de sécurité informatique et qui constituent un gibier de choix pour bon nombre de hackers, ne serait-ce que pour se marrer un bon coup. *« Vous allez entrer dans un des environnements les plus hostiles au monde »*, prévient ainsi la responsable communication de BlackHat, qui recommande aux néophytes d'éteindre les fonctions Wifi et Bluetooth sur tous leurs appareils lorsqu'ils sont sur place.

## Préférer le papier et le crayon

Il est également conseillé d'avoir des étuis anti-ondes pour protéger les cartes bancaires NFC, les passeports RFID et autres badges communicants. L'usage des distributeurs d'argent à proximité du lieu de conférence est fortement déconseillé. Il est prudent de couvrir les caméras intégrées des terminaux mobiles et PC portables par une bande adhésive opaque et de brancher ses écouteurs, pour éviter de se faire espionner en son et en image. Les chargeurs USB gratuits sont à éviter, car *« ils peuvent aspirer toutes les données d'un smartphone »*, prévient-on chez Defcon.

Bien sûr, il ne faut jamais accepter un cadeau d'un inconnu, par exemple une clé USB. Enfin, le meilleur moyen de protéger ses données sensibles, c'est encore de les laisser chez soi à la maison. *« Beaucoup de visiteurs se dotent d'ordinateurs et de téléphones à usage unique, juste pour cet évènement »*, précise-t-on chez Defcon qui recommande comme alternative au matériel informatique... un bloc-notes et un stylo, outils pour lesquels *« aucune attaque par accès distant n'est connue à ce jour »*. Arf, arf.

## Une grande variété de sujets

Une fois toutes ces consignes appliquées, le visiteur pourra alors enfin jouir des nombreuses conférences qui, cette année encore, promettent d'être particulièrement intéressantes. A BlackHat, des consultants de Qualys donneront des détails croustillants sur le contrôle de sécurité dans les aéroports et la prise de contrôle d'appareils domestiques. Deux chercheurs

@01net sur twitter

à lire aussi

SUR LES MÊMES THÈMES

- Black Hat 2014: une porte dérobée dans deux milliards de téléphones mobiles
- Black Hat: L'USB victime d'une faille de sécurité béante et impossible à corriger
- La Russie demande à Apple et SAP de lui fournir le code source de leurs produits
- Israël : le Dôme de fer piraté par la Chine?
- Etude : 80% des objets connectés mettent en danger votre vie privée
- Une faille permettait de prendre le contrôle de 99% des smartphones Android
- L'Europe prépare une force d'action contre le cybercrime
- La Russie veut-elle la peau de Tor ?
- A quoi servent les étranges portes dérobées découvertes dans les iPhone ?
- La Tesla Model S hackée lors d'un concours de sécurité
- Des milliers de LiveBox Orange piratées par un détournement de DNS
- Amazon au service de la CIA et de la NSA
- Cartes bancaires : 20 fois plus de fraudes sur Internet qu'en magasin
- L'édifiant arsenal des espions britanniques pour manipuler les contenus sur le Web
- Projet Zero : Google ouvre la chasse aux failles zero day avec une unité d'élite
- CNET.com hacké pour sensibiliser le web aux questions de sécurité ?
- Smartphone d'occasion : vous vendez vos données personnelles sans le savoir
- Silent Circle lance des forfaits de voix sur IP chiffrée
- La base de données des fonctionnaires américains, piratée depuis la Chine

d'Accuvant Labs vont montrer une porte dérobée qui concerne deux milliards de téléphones mobiles. Une série de failles iOS seront également analysées par des chercheurs de l'université de Georgia University. Deux chercheurs en sécurité allemands vont dévoiler la mauvaise sécurité des interfaces USB.

A Defcon, les conférences sont traditionnellement plus enjouées et moins « politiquement correctes ». Cette année, les hackers vont montrer l'avancement du projet NSA Playset, qui consiste à reproduire les outils de la célèbre agence de renseignement par rétro-ingénierie. D'autres montreront comment court-circuiter les pare-feux en 20 secondes, attaquer des BIOS, manipuler les systèmes de régulation de trafic routier, hacker des voitures, bloquer des ascenseurs ou, tiens pourquoi pas, pirater un mainframe IBM. Ce sera également l'occasion pour Ladar Levison et Stephen Watt de présenter l'état actuel du projet d'email sécurisé Dark Mail.

envoyer par mail imprimer l'article Tweet

Suivre @01net

Actu précédente

Black Hat 2014: une porte dérobée dans deux milliards de téléphones mobiles

01net

CGV - Conditions d'abonnement - Charte de confiance - Recrutement - Contacts - Mentions légales et CGU

NextInteractiveMedia : 01net - RMC - RMC SPORT - RMC DÉCOUVERTE - BFMTV - BFM BUSINESS - 01Business - Association RMC/BFM

Bons plans et codes promo high-tech - Code promo priceminister - Code promo mistergooddeal

lecharger.com OK GUIDE D'ACHAT ASTUCES